

THE FINANCIAL SERVICES ROUNDTABLE

BITS
FINANCIAL SERVICES
R O U N D T A B L E



19

October 14, 2003

Communications Division
Public Information Room, Mailstop
Office of the Comptroller of the Currency
250 E Street, S.W.
Washington, D.C. 20219
Attention: Docket No.

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, D.C. 20552
Attention Docket No.

Ms. Jennifer J. Johnson
Secretary
1-5
Board of Governors of the
Federal Reserve System
20th Street and Constitution Ave., N.W.
Washington, D.C. 20551
Docket No.

Robert E. Feldman
Executive Secretary
Attention: Comments/OES
Federal Deposit Insurance
Corporation
550 17th Street, N.W.
Washington, D.C. 20429

Re: Interagency Guidance on Response Programs for Unauthorized Access to
Customer Information and Customer Notice

Dear Sirs and Madams:

The Financial Services Roundtable and BITS appreciate the opportunity to comment to the Board of Governors of the Federal Reserve System (the "Board"), the Federal Deposit Insurance Corporation ("FDIC"), the Office of the Comptroller of the Currency ("OCC"), and the Office of Thrift Supervision ("OTS") (collectively, the "Agencies") on the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (the "Guidance").

The Financial Services Roundtable is a national association that represents 100 of the largest integrated financial services companies providing banking, insurance, investment products, and other financial services to American consumers. BITS is

a nonprofit industry consortium that shares its membership with The Financial Services Roundtable. BITS serves as the strategic "brain trust" for the financial services industry in the e-commerce, payments and emerging technologies arenas and also facilitates cooperation between the financial services industry and other sectors of the nation's critical infrastructure, government organizations, technology providers and third-party service providers.

The proposed Guidance supplements the statutory requirements in Section 501(b) of the Gramm-Leach Bliley Act ("GLBA") in which Congress directed the Agencies to establish standards for safeguarding customer information. The proposed Guidance, published as an Appendix to the security guidelines created under GLBA, requires financial institutions to develop programs to respond to incidents of unauthorized access to customer information and includes procedures for notifying customers under certain circumstances.

The Roundtable and BITS commend the Agencies for their continued focus on ensuring that GLBA functions properly in the marketplace, and adequately safeguards customer information. The Roundtable and BITS firmly believe that protecting customer information is of paramount concern and our member institutions have taken a proactive approach in this regard. The financial services industry's commitment is demonstrated by the development of voluntary industry guidelines relating to identity theft. In July 2003, the Roundtable and BITS announced a program entitled, "Fraud Reduction Guidelines: Strategies for Identity Theft Prevention and Victim Assistance," which provides for a "single point of contact" at companies for victims to report cases of identity theft and the use of a Uniform Affidavit for recording the victim's information about the crime. Part of this program involves the development and implementation of a twelve month pilot program to test an Identity Theft Assistance Center ("ITAC"). ITAC will assist victims of identity theft recover their financial identities.

Generally speaking, the Roundtable and BITS member companies believe that financial institutions should be given the opportunity to develop their own risk-based approach toward dealing with unauthorized access to customer information within the current guidelines set forth in section 501(b) of the GLBA. With that said, the Roundtable and BITS respectfully offer following comments in relation to the proposed Guidance:

- Section 501 (b) of the GLBA Already Provides Adequate Standards for Safeguarding Customer Information
- The Proposed Guidance Is Too Prescriptive. Financial Institutions Should Be Allowed to Take a "Risk-Based" Approach on Customer Notification
- Notice to Regulators Should Only Occur When the Incident Poses Significant Risk of Substantial Harm to a Significant Number of Customers

- Notification Delays Should Be Allowed for Law Enforcement Purposes
- Financial Institutions Should be Given More Flexibility in Determining a Course of Action When They Flag and Secure Accounts That Have Been Threatened
- Customer Notice Should be Given in a Manner Determined by the Financial Institution
- There Are Significant Burdens Imposed by the Content of the Customer Notice That Should Be Addressed
- Customer Notice Should Only Apply to Sensitive Customer Information under the Control of a Financial Institution
- The Definition of Sensitive Customer Information Needs to be Reviewed
- The Guidance Should Have the Same Geographic Scope as the GLBA
- State Laws Should Be Preempted for Institutions Covered By the Proposed Guidelines

Section 501 (b) of the GLBA Already Provides Adequate Standards for Safeguarding Customer Information

The Roundtable and BITS believe that there is no need for additional regulation in the area of customer notification. Section 501(b) of the GLBA already provides standards for safeguarding customer information. In addition, if the proposed Guidance is a response to identity theft and fraud issues in the marketplace, the financial services industry has taken a proactive approach in this area. Financial institutions have created their own comprehensive response programs to secure customer information. As discussed above, the members of the Roundtable and BITS are developing a twelve month pilot program to test an Identity Theft Assistance Center ("ITAC"). This type of innovation is an example of why an overly prescriptive rule is an inappropriate approach toward creating response programs to unauthorized access to customer information.

The Proposed Guidance Is Too Prescriptive. Financial Institutions Should Be Allowed to Take a "Risk-Based" Approach on Customer Notification

In general, the proposed Guidance is too prescriptive in listing the requirements for financial institution response programs. The Roundtable and BITS members strongly believe that the regulators should adopt a "risk-based" approach and avoid delineating specific or pre-determined requirements for notifying customers and regulatory agencies. The Roundtable and BITS members urge the regulators to be flexible and allow institutions to rely on customer notification programs that are appropriate given the risk and impact to customers and financial institutions, and that make sense within the context of existing customer relationships. Accordingly, we recommend a more flexible, less prescriptive customer

notification requirement, given the nature and variety of potential security incidents and the potential impact on customers and financial institutions.

The Roundtable and BITS believe that the proposed Guidance should include language requiring a financial institution to establish a security program that is appropriate based on the risks and the likelihood of harm to the customer. Financial institutions should be allowed to utilize their internal risk management skills to develop their own plans and programs to comply with section 501(b) of the GLBA as they see fit. As previously stated, the industry has been proactive in creating comprehensive response programs and will continue to meet the needs of their customers on an ongoing basis.

Notice to Regulators Should Only Occur When the Incident Poses Significant Risk of Substantial Harm to a Significant Number of Customers

In Section II.B of the Appendix to the proposed Guidance mandates that an institution should promptly notify its primary federal regulator when it becomes aware of an incident involving unauthorized access to or use of customer information that could result in substantial harm or inconvenience to its customers. Access that could result in inconvenience is, in our opinion, an unacceptably low threshold. Under this standard, virtually every incident may require notification. Almost any incident could possibly result in substantial harm to a financial institution's customers. While the Roundtable and BITS understand and agree that regulators should be informed of significant incidents, notification should only occur when an incident poses a significant risk of substantial harm to a significant number of its customers.

The Roundtable and BITS recommend revising the notification of primary regulator standard in Section II.B of the Appendix to read as follows:

"The institution should promptly notify its primary Federal regulator when it becomes aware of an incident involving unauthorized access to or use of customer information that poses a significant risk of substantial harm to a significant number of its customers."

Furthermore, the Roundtable and BITS recommend that the Guidance provide further clarification for the term "significant risk of substantial harm" so that financial institutions can fully understand the standard that needs to be taken into account when performing a risk-based analysis.

Notification Delays Should be Allowed for Law Enforcement Purposes

The proposed Guidance has an explicit provision for notifying law enforcement. It does not, however, contain a provision permitting institutions to take into account the interests of law enforcement when deciding when and how to provide notice. Again, a risk-based approach should apply. In general, the Agencies should be flexible in allowing institutions to deal with law enforcement and permit financial institutions to delay notification if such notification would compromise an investigation.

The Roundtable and BITS also note that an institution should not be required to obtain a formal determination from a law enforcement agency which states that notice will not compromise an investigation. This type of formal determination is required under California law (See generally, SB 1386).

Financial Institutions Should be Given More Flexibility in Determining a Course of Action When They Flag and Secure Accounts That Have Been Threatened

To provide the flexibility that financial institutions need in taking a risk-based approach toward flagging and securing accounts, the Roundtable and BITS suggest changing the language in the beginning of the Appendix, Sections II.D.1 and II.D.2 to include the words "where appropriate" to identify those situations where a company should either flag or secure accounts.

The proposed Guidance requires that a financial institution must secure an account and all other accounts that can be accessed using the same account number or name and password combination until such time as the institution and the customer can agree on a course of action. The Roundtable and BITS believe that this requirement for customer assent in Section II.D.2 of the Appendix is overly broad and should be eliminated. Such guidance does not take into account that an institution may have followed a course of action for which customer consent is not typically required or requested. The proposed Guidance should not impose a new obligation in this area. If a new customer consent requirement is imposed, it will be burdensome and a disincentive to innovative attempts by institutions to try new mechanisms for securing accounts. There would be a high operational impact on financial institutions if they had to notify or communicate with all customers or groups of customers that might be impacted from a security breach and then ask the customers if they agreed with a particular course of action. In addition, it might be operationally difficult to comply with footnote 16, which says financial institutions "should also consider" the use of new account numbers and new PINs for every affected customer.

Some of the corrective measures, such as shutting down particular applications or third party connections, might have much more serious consequences on the markets and the customers' well being than keeping the application running, as an example. This needs to be considered on a case-by-case basis and should be subjected to a risk analysis prior to taking action.

Customer Notice Should be Given in a Manner Determined by the Financial Institution

1. Notice Requirements

The Roundtable and BITS recommend flexibility in the area of customer notice. Under the section in the proposed Guidance entitled, "Examples When Notice May Be Given," the first sentence should be changed from "An institution should notify..." to "An institution should *consider* notifying..." Financial institutions should be allowed to consider whether or not the notice given to customers would provide a meaningful opportunity to help prevent or reduce the harm to those customers and/or the institution.

2. Time Period to Produce Customer Notification

The Roundtable and BITS believe that the estimated time period to develop and produce notices described in the proposed Guidance (twenty hours) and the determination as to which customers should receive notice along with the act of notification (three business days) is too low. Identification and resolution of security incidents may take significantly longer than the period of time estimated in the proposed Guidance. In considering the time to implement the proposed Guidance, the agencies should consider that the prescriptive nature of the requirements may result in significant changes to operations. Furthermore, financial institutions need time to investigate, remediate and monitor the situation to determine whether a breach has resulted in any fraud that would affect the consumer. There must be time to work with law enforcement officials to investigate the situation. And, institutions should also be given time for their own internal investigations into possible fraud.

The Roundtable and BITS recommend that the proposed Guidance include language indicating that institutions be given as much time as necessary to determine the scope of an incident and examine which customers may be affected.

The Roundtable and BITS recommend that the proposed Guidance allow the institution the opportunity to assess the risk. We propose a provision which states that customer notification, when required, may be delayed (a) to determine an occurrence of fraud, (b) to adequately investigate and assess the risk to the

customer, (c) to complete remediation of any known vulnerability, and (d) if law enforcement indicates to a financial institution that notification could compromise an on-going investigation.

3. Determining Which Customers to Notify When There is a Breach

The Roundtable and BITS believe Section II.D.3, which describes which customers are to be notified, casts too wide a net. According to the proposed Guidance, if an institution can not identify precisely which customers are affected, it should notify each customer in groups likely to have been affected, such as each customer whose information is stored in the group of files in question. The Roundtable and BITS suggest narrowing this standard by revising the end of the last sentence in the first paragraph of Section II.D.3 of the Appendix so that it reads as follows:

"However, if the institution cannot identify precisely which customers are affected, it should notify each customer in groups likely to have been affected such as each customer whose information is stored in the group of files in question, assuming the parameters described in Paragraph III ("Circumstances for Customer Notice") are met."

As previously discussed, the need for flexibility in this area is great. The costs associated with a widespread and unwarranted notice may be significant. Unnecessary notice to customers creates undue anxiety for customers and reputational risk and operational difficulties for financial institutions.

4. Delivery of Customer Notice

Flexibility is not only important in determining whether notice should be provided in a given case, but it is also important in the consideration of the manner of delivery. Section II.D.3 of the Appendix sets out the correct standard by indicating that notice should be timely, clear and conspicuous and delivered in any manner that will ensure that the customer is likely to receive it. In addition, the Roundtable and BITS believe that the proposed Guidance properly permits electronic notice for those customers who conduct transactions electronically and wisely refrains from requiring institutions to deliver notices by more than one means.

There Are Significant Burdens Imposed by the Content of the Customer Notice That Should Be Addressed

The Roundtable and BITS believe that the proposed Guidance should not overlook the impact and burden of notification on customers as well as institutions. As

currently constituted the proposed Guidance calls for notice to all customers or groups of customers whenever there is some chance they may be affected.

1. Adverse customer reaction

Every notice to customers may cause anxiety on the part of customers. Financial institutions may not be able to adequately respond to customers' inquiries about the likelihood of financial loss resulting from an identity theft. As a result, customers may unnecessarily change passwords, cancel accounts or take other actions after receiving a notification. Perhaps more importantly, initial customer overreaction may ultimately breed customer under reaction. If notice is not tied to risk, customers may under react to notices, become less responsive and fail to take the necessary action at the appropriate time. Also, customers receiving frequent notices from financial services institutions may become inured to them, ultimately becoming less responsive to the most serious threats.

To address the burdens imposed by the proposed Guidance in the area of customer notice, the Roundtable and BITS suggest the following language:

"An institution should notify affected customers whenever it becomes aware of unauthorized access to sensitive customer information under its control unless the institution reasonably concludes that misuse of the information is unlikely to occur or the burden of notification on the customer and the institution outweighs the value of individual customer notification. If an institution concludes that notice is not required, it shall take appropriate steps to safeguard the interests of affected customers, including, where appropriate, monitoring affected customers' accounts for unusual or suspicious activity."

2. Costs

Certain aspects of the customer notice set forth in Section II.D.3.b may increase financial institutions' costs dramatically. There are tangible costs associated with delivery of a notice (whether by phone, mail, or email). If an incident affects a large portion of the customer base of the typical financial institution or even a large portion of the customer base for some products of an institution, the costs could be enormous. In addition, the costs of meeting the requirements of footnote 17 (requiring a sufficient number of appropriately trained employees to be available to answer customer inquiries and provide assistance) could also be substantial.

A less prescriptive model for customer notices would alleviate the financial and practical burden that the proposed Guidance will impose upon institutions. In particular, the Roundtable and BITS strongly recommend:

- Changing Appendix Section II.D.3, from “Key elements: In addition, the notice should:” to “Key elements: the notice should, where appropriate:”
- Not mandating a specific time period, but more flexible time periods, where appropriate.
- Deleting the requirement to inform affected customers that the institution will assist the customer to correct and update information in any consumer report relating to the customer. Requiring financial institutions to add this information in their notice to customers goes beyond the requirements of the Fair Credit Reporting Act (“FCRA”) and imposes a potentially costly obligation on financial institutions because of the individual customer inquiries that such a notice might trigger.
- Deleting the “Optional Elements” in Section II.3. The Roundtable and BITS do not believe that inserting these elements into the proposed Guidance will serve any useful purpose and may instead result in elements that are not perceived as optional, by customers or institutions. Many of these “elements” are onerous, costly and inappropriate in a number of circumstances. While financial services institutions may offer these services under certain circumstances, they should not be included in the proposed Guidance. For example, the suggestion that an institution “offer” to assist a customer in notifying the nationwide credit reporting agencies of an incident and further “offer” to assist customers in placing a fraud alert in the customer’s reports, is an example of a highly costly element that should be left outside the scope of the proposed Guidance.

The arguments set forth above also apply to the suggestion in the “Optional Elements” section of the proposed Guidance that an institution “offer to subscribe” a customer to a subscription service free of charge for a period of time (these subscription services provide customers notification of requests that have been made for a customers’ credit report). The Roundtable and BITS strongly believe that this suggestion is misplaced in the proposed Guidance and should be deleted.

Customer Notice Should Only Apply to Sensitive Customer Information under the Control of a Financial Institution

Customer notice should only apply to sensitive customer information under the control of a financial institution. Where the institution has contracted with a third party to carry out some or all of its information technology functions, the institution continues to control the sensitive customer information and should provide any notification. However, where the financial institution provides

sensitive customer information to federal, state or local government entities, and that entity suffers a security breach, the financial institution should not be required to notify customers of such an incident. The proposed Guidance should make clear that once the information is sent to a government entity, for example, the information is no longer under the control of the financial institution. The Roundtable and BITS also note that this clarification should focus on the "control" of information rather than the ownership of information because, in any given situation, ownership of sensitive customer information may be less clear than control of the information.

The Definition of Sensitive Customer Information Needs to be Reviewed

Certain aspects of "sensitive customer information" need to be further scrutinized. A key element to this definition is whether or not particular information materially increases the likelihood that a particular consumer would become the victim of identity theft or fraud. The Roundtable and BITS have the following recommendations:

1. "Encrypted information" should not be considered sensitive information. If customer information is encrypted, no notification should be required. Not including encrypted data in the definition of sensitive customer information may motivate companies to continue efforts to encrypt sensitive data. Financial institutions should consider whether or not the data is encrypted when conducting their risk-based analysis of whether or not the customer will be harmed.
2. "Account numbers" by themselves should not be considered sensitive information. For example, the account number for an installment loan is of no use to potential hackers. Often, account numbers without access codes or expiration dates are useless unless the account can be debited without any access code or device. This should be addressed in the proposed Guidance by only including that information which could lead to access to a customer's financial information or the ability to initiate a transaction in the customer's account.
3. "Publicly available information", defined as information that is lawfully made available to the general public from federal, state, or local government records, should also be excluded from the definition of sensitive data.

There is a need to define *customer information* more specifically versus *sensitive customer information*. It is clear that names and addresses are customer information, but are there other items included in this category? This is important because certain actions are required when, for example, someone with access to customer information (not necessarily sensitive customer information), needs to have a background check. There should probably be an all-inclusive list of

customer information and then some criteria as to what might be considered sensitive. In terms of identifiers, information that is unique to a person might be the most sensitive, *e.g.*, SSN, mother's maiden name, *etc.* The Roundtable and BITS believe more clarification is needed in this area.

The Guidance Should Have the Same Geographic Scope as the GLBA

The proposed Guidance does not expressly set forth the scope of its application. Because the proposed Guidance is intended to relate back to the Gramm-Leach-Bliley Act, the scope of the proposed Guidance should be no greater than those regulations. The relevant regulations are limited to the "United States offices" of entities subject to the relevant federal financial regulator. See, *e.g.*, 12 C.F.R. 40.1(b)(1). The current document should similarly reflect this limitation, making it clear that foreign offices, affiliates, and branches of U.S. financial institutions are not subject to the proposed Guidance.

State Laws Should Be Preempted for Institutions Covered By the Proposed Guidelines

The Agencies should indicate that state laws, such as SB 1386, are preempted for institutions covered by the proposed Guidelines. The practical effect will be that such institutions would not be required to give a notice if there is a determination that there has not been, and is not likely to be, misuse of the information and e-mail notification would be permissible when individual notice is required, even if the institution does not have E-SIGN level consent (*i.e.*, the institution has obtained consent from the consumer in a form that demonstrates that he or she is able to receive information electronically). Preemption would also avoid ambiguities in the California law, such as whether non-California individuals can be counted in determining whether the threshold for substitute notice has been met. And finally, preemption would eliminate confusion to customers who may get conflicting notices from financial institutions.

Conclusion

The Roundtable and BITS strongly urge the Agencies to circulate another draft of the proposed Guidance. We believe that these significant changes should not proceed without more careful consideration of the many issues raised in this response and in the responses to be submitted by other firms and industry associations.

The Roundtable and BITS suggest that the Agencies consider forming an advisory group of the firms most directly impacted by the proposed Guidance in order to

gather further intelligence and a better understanding of the practical aspects of implementing these rules.

Finally, when and if the proposed Guidance is finalized, it should include a specific provision allowing adequate time for institutions to implement the requirements outlined.

If you have any further questions or comments on this matter, please do not hesitate to contact us or John Beccia at (202) 289-4322.

Sincerely,

A handwritten signature in cursive script that reads "Catherine A. Allen".

Catherine A. Allen
CEO, BITS

A handwritten signature in cursive script that reads "Richard M. Whiting".

Richard M. Whiting
Executive Director and General Counsel
The Financial Services Roundtable